Chapter 1 – Introduction and Overview

The Information Security Framework document establishes security objectives, controls and practices for Indiana state government. It also establishes minimum compliance activities to assure practices are effective in accomplishing their security control objective. The security objectives and controls apply to all hardware, software, data, information, network, personal computing devices, support personnel, and users within State agencies. Going forward, these components of information technology are covered by the umbrella term of "information resources."

The State of Indiana Information Security Framework (ISF) replaces the Information Security Policies & Minimum Compliance Requirements that previously provided information security guidance. The State of Indiana's Information Framework follow the ISO 17799 standard. This document maintains the consistency of the ISO 17799 numbering scheme. Doing so makes the ISF consistent with and, for those familiar with the ISO 17799 standard, very easy to use. However, those unfamiliar with the standard may find navigation less intuitive.

To maintain a numbering scheme consistent with ISO 17799 chapters, information common to introductions appears in Chapter 5 – Security Policy. For a quick understanding of the organization of this document see the chapter overview below.

Overview of Chapters

Chapter 2 – Scope: A brief look at the scope of this document. It is brief due to the detail provided in Chapter 5 – Security Policy.
Chapter 3 – Definitions: A straightforward look at the terms used in this document.
Chapter 4 – Risk Assessment and Treatment: Documents the process the state will use to identify and assess risk as well as treat the risk through controls and practices.
Chapter 5 – Security Policy: Discusses the scope of policy, as well as roles and responsibilities.
Chapter 6 – Organizational Security: Addresses security around the workforce, third parties, and outsourcers.
Chapter 7 – Asset Classification and Control: Assures appropriate protection of state physical assets.
Chapter 8 – Human Resources Security: Addresses the considerations with state workforce members prior to employment, during employment, and after termination.
Chapter 9 – Physical and Environmental Security: Deals with the protection of physical areas and equipment from physical threats and unauthorized access.
Chapter 10 – Communications and Operations Management: Addresses the many facets of information technology operations.
Chapter 11 – System Access Controls: Tackles access restrictions for users at network, operating system, application and mobile computing levels.
Chapter 12 – System Development and Maintenance: Deals with the many aspects of application development and maintenance security concerns.
Chapter 13 – Information Security Incident Management: Discusses the reporting and management requirement for security incidents.

Chapter 14 – Business Continuity Management: Plans for interruptions of state of Indiana business activities.
Chapter 15 – Compliance: Addresses the states compliance with laws and statutes, security policies, controls and practices as well as audit considerations.

The comprehensive ISO framework is a good fit for the diverse missions of Indiana state agencies. Following the ISO format results in comprehensive coverage of the different security issues faced by agencies. A three tiered approach addresses nearly every security concern State agencies face. The three tiers consist of control objectives, controls, and practices. The three tiers of the ISF are best explained through an example.

Document Format Example:

7.2 Information classification
Owners classify their information assets with regard to Confidentiality, Integrity, and Availability. Classifications drive the specific levels of protection applied.

Control 7.2.1 – Standardized information classifications apply to information assets and require regular review.

Practice 7.2.1.1 - Confidentiality classification scheme
Practice 7.2.1.2 – Availability classification scheme

Control 7.2.2 – The classification system determines authorizations to see the information, labeling requirements, disposal requirements, and encryption requirements.

Three-tier Breakdown

Control Objective Level

At the control objective level, the state identifies the security objective for the particular topic. There are currently 42 security control objectives. Below, **7.2** represents the control objective number and **Information classification** the control objective title.

7.2 Information classification
Owners classify their information assets with regard to Confidentiality, Integrity, and Availability. Classifications drive the specific levels of protection applied.

Control Level

Controls state the requirements to meet the objective. There are currently 138 controls in this document. In the example there are 2 controls for the control objective.

Control 7.2.1 – Standardized information classifications apply to information assets and require regular review.
Control 7.2.2 – The classification system determines authorizations to see the information, labeling requirements, disposal requirements, and encryption requirements.

Practice Level

Practices get very specific on how the controls are accomplished. Not every control will require a practice while others will require more than one. Below, there are two practices applicable to Control 7.2.1 while there are currently none for Control 7.2.2. The practice name will link to the actual practice.

Practice 7.2.1.1 - Confidentiality classification scheme
Practice 7.2.1.2 – Availability classification scheme

Chapter 2 – Scope

The control objectives and controls, as well as many practices included in this document, apply to all executive branch agencies, their employees and contractors, and the information they use in the performance of their duty on behalf of the citizen. They apply to all hardware, software, data, information, network, personal computing devices, support personnel, and users within State Agencies.

In addition to the executive branch of government workforce members, these requirements apply to any party that will use or put at risk executive branch information resources, through the execution of their duties.

Chapter 3 – Terms and Definitions

Definitions of terms found in this document and general security terms can be found at this link:

Chapter 4 – Risk Assessment and Treatment

4.1 Assessing Security Risk

Information systems and other important technology assets undergo risk assessments. Remediation is the shared responsibility of IOT Security and the agency owning the information asset.

Control 4.1.1 – The state of Indiana uses a standard risk assessment methodology.

Practice 4.1.1.1 – Risk assessment process, information technology

Control 4.1.2 – The assessment methodology is consistently repeatable and applied by all state agencies.

Control 4.1.3 – Risk assessments occur at regular intervals determined by threats and risk levels, identification of new risks, or with environmental changes requiring reassessment.

Control 4.1.4 – Risk assessments include a defined scope (enterprise, agency specific, system specific, component specific) and assign and agree to ownership.

4.2 Treating Security Risks

Agencies are accountable for assuring the development and execution of remediation plans and the ongoing monitoring of risks to assets they own. Risk treatment plans must include the scope and mitigation actions and controls. The CISO's office files results on-line.

Control 4.2.1 – Treatment plans include the requirements for risk remediation.

Control 4.2.2 – Asset owner provides annual assessments of the risk treatment's effectiveness, consider the treatment's efficiency, and implement improvements.

Control 4.2.3 – The asset owner identifies the means for measuring effectiveness of controls.

Control 4.2.4 – The owner confirms identified controls have appropriate risk reduction/cost ratios.

Control 4.2.5 – Design stages consider security controls requirements.

Chapter 5 – Security Policy

5.1 – Security Policy

Development, maintenance, and compliance monitoring of the State of Indiana's information security policy is the responsibility of the Chief Information Security Officer (CISO) of the Office of Technology (IOT). The primary goal of these policies is to protect information commensurate with sensitivity levels. The public rightly assumes the data in the possession of state government is secure and protected from unauthorized access and modification. In addition to the protection of citizen information, the policies established intend to protect the state's fiscal investment in resources which include computer resources, communications resources, and human resources.

Each agency must formally delegate responsibility for all information security matters. Multiple individuals across organizational lines may be involved as long as there is a clear separation of duties and responsibilities which provide effective checks, balances and accountability

State security policies reinforce the following important concepts:

- Ensuring the confidentiality, integrity of information, and availability of Information Resources is a critical function of state government.
- Recognizing that information security reflects a "business of government" need and not just a technology need.
- Establishing a core understanding that Workforce Members share accountability for information security.
- Promoting the appropriate balance of security risk levels and cost of risk mitigation and disaster recovery.
- Promoting an enterprise-wide understanding of, and responsibility for, information security.
- Ensuring information security requirements include both in-house and outsourced resources.
- Establishing formal processes for reviewing and approving individual waivers and policy exceptions before implementation.

IOT's Information Security area will prepare, maintain, and publish an information security policy manual that concisely describes the state's information security policies and procedures.

Control 5.1.1 – All state of Indiana information security policy is contained within this document, its practices, attachments, and appendices.

Practice 5.1.1.1 – The Information Resources Use Agreement (IRUA).

Control 5.1.2 – The Office of Technology's Chief Information Security Officer (CISO) owns all control objectives, controls, and practices included in this document subject to proper socialization among State business and IT leaders. Reviews occur regularly, in the event of security incidents, and with the identification of new vulnerabilities. Reviews document findings and desired actions.

Chapter 6 – Organizational Security

6.1 Information Security Infrastructure

IOT, through the Chief Information Security Officer, will allocate and/or coordinate sufficient resources to adequately address the information security function required by the State of Indiana. The Information Security organization of IOT is responsible for providing methods for securing information and its supporting resources. It is the responsibility of workforce members and agents of the state to communicate their security requirements for the protection of information to the Information Security organization.

Control 6.1.1 – The CISO owns, updates and educates on the materials covered in the ISF. Responsibilities include:

- Regular reviews of policy and controls
- Regular review of security responsibilities
- Monitoring significant changes in the exposure of information assets to major threats
- Regular reviews and monitoring of information security incidents
- Regular reviews of exposure to threats
- Approve initiatives for enhancing information security
- Inclusion of appropriate resources in the development of, changes to, and implementation of control objectives, controls, and practices.

Control 6.1.2 – The CISO will coordinate protection activities for the executive branch of state government including all information assets, hardware assets, and software assets.

Control 6.1.3 – All production information possessed by or used by an organizational unit must have a designated owner whose responsibilities include determining appropriate sensitivity classifications, criticality ratings, and access controls over the use of this information.

Practice 6.1.3.1 – Information asset ownership definition and requirements

Control 6.1.4 – All information assets, including new systems, use appropriate procurement and review mechanisms as established by the Indiana Department of Administration.

Control 6.1.5 – Information security expertise is available or purchased, by the agency or IOT, as needs dictate.

Control 6.1.6 – The state of Indiana appropriately interacts with external security contacts and organizations as needed to protect citizen information.

Practice 6.1.6.1 – Security contact list

Practice 6.1.6.2 – Security group participation list (states, local)

Control 6.1.7 – Independent audits of the State of Indiana information security program evaluate effectiveness every 2 years.

6.2 Security of third party access

Third parties gain access to state information assets only where there is a business need, only with approval of system owners, and only with the minimum access needed to accomplish the business objective.

Control 6.2.1 – Third parties accessing the system are subject to the contents of this document, must agree to the terms of the Information Resources Use Agreement (IRUA), and take the required IRUA required training course.
Control 6.2.2 – Contract language should detail the security requirements of all parties involved in an agreement.

6.3 Outsourcing

System owners assure adequate protection and controls from outsourcers. Thorough risk assessments result in clear contractual requirements on the part of the outsourcer.

Control 6.3.1 – Contracts document security requirements, specific to the outsourced service. Regular audits evaluate compliance.

Practice 6.3.1.1 – Outsourcing contract review
Practice 6.3.1.2 – Outsourced security audit requirements

6.4 Agency planning

Each state agency leader must prepare an annual plan for bringing those computer and communications systems within their area of responsibility into compliance with published security policies and controls. It is a primary function of the state agency leaders to make a specific decision about the degree to which the state will institute controls to reduce or mitigate losses for every significant information system's security risk.

Consider need after consolidation.

Chapter 7 - Asset Classification and Control

7.1 Accountability for assets

Every information asset has an owner specified by agency management. The owner protects the asset by implementing proper controls.

Control 7.1.1 – A statewide inventory maintains information asset information clearly identifying the asset and its owner. Risk assessments result in documentation of the following:

- Security classification
- Severity and likelihood of risks
- Required controls
- Acceptance of remaining risks
- Necessary operational procedures
- Authorized access
- Reports, tapes, etc. require classification labels.

7.2 Information classification

Owners classify their information assets with regard to Confidentiality, Integrity, and Availability. Classifications drive the specific levels of protection applied.

Control 7.2.1 – Standardized information classifications apply to information assets and require regular review.

Practice 7.2.1.1 - Confidentiality classification scheme

Practice 7.2.1.2 – Availability classification scheme

Control 7.2.2 – The classification system determines authorizations to see the information, labeling requirements, disposal requirements, and encryption requirements.

Chapter 8 - Human Resources Security

8.1 Prior Employment

All new hires undergo scrutiny proving fitness for hire. Agencies communicate security responsibilities of the position during recruitment.

Control 8.1.1 –Job descriptions include security roles and responsibilities and job performance criteria.

Control 8.1.2 – Conduct background checks as dictated by the Indiana State Personnel Department.

Control 8.1.3 – New workforce members know their security responsibilities and the consequences of failing to meet them.

Reference Practice 5.1.1.1 - The Information Resources Use Agreement (IRUA).

8.2 During Employment

All workforce members have sufficient training and supporting reference materials to properly protect state owned information assets and resources. All workforce members responsibly apply this training and support to protect the state's information assets.

Control 8.2.1 – All new hires must take a designated security training course on acceptable use prior to gaining system access.

Practice 8.2.1.1 – Information Resources Use Agreement (IRUA) Training Module

Control 8.2.2 – Workforce members receive security training to the extent required by their position. Course refreshers may be required dependent on the subject.

Control 8.2.3 – Workforce members face disciplinary actions up to and including dismissal for violations as determined by their management and the State Personnel Department.

Control 8.2.4 – Assure the necessary separation of duties necessary for auditing.

8.3 Termination or Change of Employment

Immediate managers are responsible for timely notification of terminated employees and those changing roles to the appropriate technical support organizations.

Control 8.3.1 – Human resources notifies technical support of security responsibilities following the former workforce member after employment.

Control 8.3.2 – Assure the return of all information assets in the possession of a terminated workforce member. Evaluate all services used by the terminated workforce member for need of continuation (e.g. – phone, cell phone, pager, etc.).

Control 8.3.3 – Revoke the rights to all systems of a terminated workforce member, or one changing role, without delay.

*Control 8.*3.4 – Evaluate terminated employee computer-based and paper files for disposition.

Chapter 9 - Physical and Environmental Security

9.1 Secure areas

Protection of physical areas is consistent with the critical or sensitive business information stored in the area regardless of format (printed, digital).

Control 9.1.1 – Physical security perimeters are consistent with the value of information or services protected.

Control 9.1.2 – Entry controls and access rights are at minimum levels for successful service execution. Revoke all access rights immediately for staff changing roles.

Control 9.1.3 – IT facilities supporting critical or sensitive business activities have adequate physical security.

Control 9.1.4 – Workers in secure areas receive training on procedures. Third party access is minimized and monitored.

Control 9.1.5 - Delivery loading areas for data centers are isolated and enable inspection of deliveries.

Control 9.1.6 – Keys and access badges to secured areas are controlled ensuring only authorized personnel gain access.

9.2 Equipment security

Equipment is secured from physical threats and unauthorized access.

Control 9.2.1 – Equipment requiring special protection is isolated.

Control 9.2.2 – Protect equipment from power failures and surges.

Control 9.2.3 - Cabling is protected from interception and physical damage.

Control 9.2.4 – Maintain IT equipment per manufacturer recommendations with service completed only by authorized providers.

Control 9.2.5 – Protection levels for IT equipment used inside and outside the primary premises are the same.

Control 9.2.6 – Destruction of obsolete and damaged storage devices follow IDOA surplus guidelines. Archiving and discarding documents is per a schedule for their classification.

Control 9.2.7 – Equipment and software moved off-site require management approval.

Chapter 10 - Communications and Operations Management

10.1 Operational procedures and responsibilities

Assure the correct and secure operation of information processing facilities through documentation of responsible parties and operating instructions.

Control 10.1.1 – Documented procedures identify responsibilities for managing and operating all computers and networks.

Control 10.1.2 – Staff follow documented change control processes.

Practice 10.1.2.1 – Patch management procedures

Control 10.1.3 – Segregation of duties reduces risks of unauthorized modification or misuse of information assets.

Control 10.1.4 – Separate development, test and operational facilities.

10.2 Third party service delivery management

Contracts and agreements document third party service delivery requirements including appropriate levels of security.

Control 10.2.1 – Third parties implement security controls set out contractually.

Control 10.2.2 – The state maintains overall control of security aspects of services provided by third parties.

10.3 System planning and acceptance

Manage systems proactively and protect them from failures.

Control 10.3.1 – Systems management processes provide capacity planning, systems acceptance criteria, emergency conditions planning, and change controls

Control 10.3.2 – Meet acceptance testing criteria. Train operations staff for any production environment changes.

10.4 Protection from malicious software

Protection schemes assure the integrity of information, software, and operating systems from malicious software.

Control 10.4.1 – Virus control procedures, virus protection software, and the prohibition of unauthorized software protect the integrity of information and software.

10.5 Backup

Backup strategies assure information integrity and availability considering inadvertent destruction, corruption, and disaster scenarios.

Control 10.5.1 –Backups schedules provide protection consistent with the information classification. Storage is secure physically and environmentally. Backup testing is regular per published schedules.

Control 10.5.2 – Regular audits monitor operator activities.

Control 10.5.3 – Identify and record faults and test to confirm no compromise.

Control 10.5.4 – Movements of backup tapes to and from storage locations is secure.

10.6 Network Management

Secure network connections assure safe transmission of information.

Control 10.6.1 – Network management assures effective network design, has clearly defined responsibilities and procedures, and is distinguished from computer operations.

10.7 Media handling and security

Media protection prevents, whether in use, storage, or transit, losses from theft, unauthorized access, and environmental hazards.

Control 10.7.1 – Media handling procedures document storage, distribution, and disposal requirements; discreet naming conventions; and any erasure parameters.

Control 10.7.2 – Data classification dictates media disposal method and logging requirements.

Control 10.7.3 – Procedures exist for the handling and storage of input/output media.

Control 10.7.4 – System documentation protection considers importance and disaster situations availability requirements.

10.8 Exchanges of information and software

Exchanges of information between the state, its workforce, and third parties consider relevant legislation, contractual terms, and other agreements assuring integrity and authorized use.

Control 10.8.1 – Formal agreements between the state and third parties assure comprehensive detailing of security controls and ownership responsibilities.

Control 10.8.2 – Transit protection prevents unauthorized disclosure and physical damage.

Control 10.8.3 – Electronic commerce transmission controls assure integrity and verify authenticity while mitigating risks of introducing malicious code.

Control 10.8.4 – Electronic mail security prevents modification. Workforce members understand appropriate use policies.

Control 10.8.5 – Conduct risk assessments on each office system and assure appropriate security controls.

Control 10.8.6 – Information published electronically complies with an authorization process and carefully protects integrity.

Control 10.8.7 – Communicate requirements to appropriate state of Indiana workforce members regarding use of voice, facsimile, and video communications.

10.9 Electronic Commerce Services

Electronic commerce systems designs and implementations carefully consider security risks as well as business requirements.

Control 10.9.1 – Defined electronic commerce terms and security controls apply to every application.

Control 10.9.2 – Information protection schemes prevent modification and unauthorized disclosure.

10.10 Monitoring

Systems monitoring safeguards unauthorized information processing activities, records events, and documents circumstances.

Control 10.10.1 – Audit logs capture user activities and security events.

Control 10.10.2 – Monitoring captures User ID activities including files accessed, programs used and unauthorized access attempts.

Practice 10.10.2.1 – Employee computer use active monitoring

Control 10.10.3 – Log storage prevents tampering and unauthorized access.

Control 10.10.4 – Logging tracks privileged access activities.

Control 10.10.5 – Faults trigger analysis and necessary actions.

Control 10.10.6 – Relevant systems have clocks synchronized.

Chapter 11 - System Access Controls

11.1 Business requirements for access control

Access granted to information is the minimum required to successfully accomplish work responsibilities.

Control 11.1.1 – Defined and documented roles drive access levels.

11.2 User access management

Systems limit access only to authorized users and to defined limitations.

Control 11.2.1 – Users have unique IDs and are educated on their access level.
Control 11.2.2 – Limited number of staff acquire special privileges with justifying documentation required. Special privileges require a different ID than one used for normal business.
Control 11.2.3 – Users change passwords at initial login, never share passwords, and change passwords securely.
Control 11.2.4 – User access rights require regular review.

11.3 User responsibilities

Training results in users understanding the importance of secure passwords and act appropriately to maintain their confidentiality.

Control 11.3.1 – Users select secure passwords and keep them confidential.
Control 11.3.2 – Users lock keyboards to prevent unauthorized access while away from their computing environment.

11.4 Network access control

Access to network resources is limited to only those services required. Limitations apply to:

- Networks outside of the primary campus network and wide area network, currently operated and maintained by IOT (both public and private),
- individual and group access to services, and
- appropriate authentication mechanisms for users and equipment.

Control 11.4.1 – Network access controls appropriately limit available services.
Control 11.4.2 – Network routing ensures only allowed paths to services are used.
Control 11.4.3 – User authentication is required for external connections.
Control 11.4.4 – Node authentication
Control 11.4.5 – Diagnostic ports access is limited and audited.
Control 11.4.6 – System security requirements dictate segregation of networks.
Control 11.4.7 – Network gateways have the necessary filters.
Control 11.4.8 – Networks have appropriate routing controls.
Control 11.4.9 – Routine audits of network services protect from security risks.

11.5 Operating System access control

Operating system security facilities assure access to computer resources is appropriate and authorized.

Control 11.5.1 – Terminal identification enables protection or auditing capabilities when required.

Control 11.5.2 – Logon processes provide degrees of protection commensurate with the security required of services.
Control 11.5.3 – All activities are traceable to individual users. Shared IDs are exceptions, approved by management, and documented.
Control 11.5.4 – Password management schemes effectively balance security requirements with ease of use.
Control 11.5.5 – Access to system utilities is limited to authorized resources.
Control 11.5.6 – Research – duress alarm for coercion
Control 11.5.7 – Inactive terminals time-out at intervals determined by the security requirements of the system.
Control 11.5.8 – Connection time restrictions limit access as required by application sensitivity levels.

11.6 Application and Information Access Control
Permit only authorized users access to information stored in applications.

Control 11.6.1 – Logical access controls appropriately limit access.
Control 11.6.2 – Sensitive systems are isolated to the degree necessary for protection.

11.7 Mobile computing and teleworking
Protective measures secure information and assets used in mobile computing or teleworking.

Control 11.7.1 – Controls and training protect information and mobile computing devices.
Control 11.7.2 – Teleworking policies are documented.

Chapter 12 - System Development and Maintenance

12.1 Security Requirements of Information Systems - Business applications and user-developed applications identify security requirements in the business process.

Control 12.1.1 – Defined security requirements drive purchasing and development decisions.

12.2 Correct Processing in Applications

Controls and audit prevent errors, loss, unauthorized modification, and misuse of information.

Control 12.2.1 – Applications have data integrity controls.
Control 12.2.2 – Checks and controls protect against data corruption.
Control 12.2.3 – Message authentication - in development
Control 12.2.4 – Data outputs validate processing is correct.

12.3 Cryptographic controls

Cryptographic systems apply protections for confidentiality, authenticity, and integrity of information considered at risk and where other controls provide inadequate protection.

Control 12.3.1 – in development
Control 12.3.2 - in development
Control 12.3.3 – in development
Control 12.3.4 - in development
Control 12.3.5 - in development

12.4 Security of System Files

IT project and support activities use appropriate controls to assure integrity and confidentiality.

Control 12.4.1 – Change control procedures protect program libraries and test data. Reviews assess effectiveness. Audit trails exist for all changes.
Control 12.4.2 – Live data when used for testing requires authorization, is de-personalized and has the same access limitations as production data. Erasure of data happens immediately upon completion of testing.
Control 12.2.3 – Access is restricted to operational source program libraries, access is auditable, and old versions archived.

12.5 Security in Development and Support Processes

Strictly controlled project and support environments enable the timely development of quality applications.

Control 12.5.1 – Apply change control procedures to development and support environments. Authorized, document, and audit changes.
Control 12.5.2 – Study operating system changes for impacts to applications and approved by application owners.
Control 12.5.3 – Make changes to off-the-shelf software applications only in compliance with licensing terms and an overwhelming business need.
Control 12.5.4 – Purchase applications only from reputable sources where confidence in source code quality is high.

Control 12.5.5 – Manage outsourced software development to assure favorable licensing terms and certification of code quality.

12.6 – Vacant

12.7 Technical Vulnerability Management

Proactively monitor published software vulnerabilities. Apply assessments to vulnerability risks and mitigation actions.

Control 12.7.1 – Monitor resources for vulnerability awareness. Evaluate and test fixes prior to moving into production.

Chapter 13 - Information Security Incident Management

13.1 Reporting information security events and weaknesses

Communicate information security incidents through documentation identifying the scope, owners of impacted information or assets, in a timely manner.

Control 13.1.1 – Document security incidents, assure adherence to incident communication procedures, and train appropriate staff on incident handling.

13.2 Management of Information Security Incidents and Improvements

Incident handling procedures enable the effective handling of incidents by appropriate levels of technical and managerial staff.

Control 13.2.1 – Incident responses are quick, organized, and effective.

Practice 13.2.1.1 – IOT computer emergency response team (CERT) (to be developed)

Control 13.2.2 – Security incidents are studied and preventative measures implemented to inhibit recurrences.

Control 13.2.3 – Procedures are in place for collecting and handling evidence for disciplinary purposes.

Chapter 14 - Business Continuity Management

14.1 Information Security Aspects of Business Continuity Management

Documented plans plan for interruptions to business activities and protect critical business process from the effects of major failures or disasters

Control 14.1.1 – Business process owners have identified their critical processes, identified their recovery requirements, and have assured recovery plans are in place.

Control 14.1.2 – Strategies for known impacts of interruptions are in place to successfully restore services in defined timeframes.

Control 14.1.3 – Business continuity plans identify parties and their roles and emergency procedures.

Control 14.1.4 – Resumption procedures consider emergency and fallback plans and testing schedules.

Control 14.1.5 – Business process owners assure that business continuity plans are tested. Documentation updates occur monthly.

Chapter 15 - Compliance

15.1 Compliance with Legal Requirements

Information systems comply with all laws, statutes, and contractual obligations.

Control 15.1.1 – Each system considers relevant statutory and contractual requirements.

Control 15.1.2 – Procedures are in place to assure compliance with statutes, licensing agreements, and intellectual property rights.

Control 15.1.3 – Procedures are in place to assure the protection of essential records. Retention schedules follow ICPR guidelines.

Control 15.1.4 – Protection of personal information meets levels required by legislation.

Control 15.1.5 –Information resources use is for authorized business purposes only.

Control 15.1.6 – Systems using cryptography comply with federal laws.

Control 15.1.7 – Evidence gathered conforms to rules of evidence assuring admissibility.

15.2 Compliance with Security Control Objectives, Controls and Practices

Information systems security reviews assure meeting control objectives and compliance with controls and practices.

Control 15.2.1 – System reviews address shortcomings through action plans.

Control 15.2.2 – Authorized personnel perform logical security tests.

15.3 Information System Audit Considerations

Information system audits safeguard information and productivity while being conducted. Use audit tools only for authorized audits.

Control 15.3.1 – Information systems owners and application owners agree on system audit scope, timing, and the resolution of discovered vulnerabilities.

Control 15.3.2 – System audit tools are stored to prevent misuse or compromise and access to the tools is controlled.